OFFICE OF THE DIRECTOR
DEFENSE RESEARCH AND ENGINEERING
3040 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-3040

August 20, 2004

MEMORANDUM FOR HPC CENTER MANAGERS; SERVICE/AGENCY APPROVAL AUTHORITIES

SUBECT: Implementation of Non-sensitive HPC Systems via the DoD HPC Modernization Program Uniform Use-Access Policy

Ref: (a) DUSD (S&T), Enhanced Security of High Performance Computing Resources, May 12, 1999
(b) DoD HPCMP, Revision to Uniform Use-Access Policy to HPCMP Resources, September 28, 2001

1. The DoD HPC Modernization Program Uniform Use-Access Policy (ref (a)) was implemented in 1999 to mitigate risk associated with providing DoD researchers and their contractor and academic affiliates access to the high performance computing (HPC) resources of the DoD HPC Modernization Program. This policy requires that all users, regardless of affiliation, be required to undergo a "trustworthiness certification" as evidenced by, at a minimum, having undergone a National Agency Check before being provided access to the sensitive but unclassified computing resources of the HPCMP. This requirement is consistent with that expressed in DoDI 5200.2-R, section C3.6.2.1.

> "Access to restricted areas, sensitive information or equipment by DoD military, civilian or contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or ENTNAC) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate DoD Component Agency or activity prior to permitting such access."

In addition, the Uniform Use-Access Policy allows for the establishment of non-sensitive HPC systems (paragraph 4.2 of ref (a)). This policy statement provides rationale for implementation of non-sensitive HPC systems within the HPCMP.

2. As a result of delays in completion, caused by a severe backlog in processing requested NAC investigations by the DoD investigative offices, the Uniform Use-Access Policy was subsequently modified to permit interim (immediate) access to the sensitive but unclassified computer resources of the HPCMP by US nationals only, upon submission (i.e., prior to the completion of the actual investigation) of a completed NAC questionnaire (ref (b)). This interim access would be declared final upon completion of the full NAC investigation.

3. The HPCMP has continuously re-examined its Uniform Use-Access Policy and its implementation to ensure it was providing minimal risk to all sensitive but unclassified HPC resources while still providing timely access to these systems. Although turnaround times on NAC processing by OPM have improved substantially, many user organizations, particularly basic researchers at academic institutions, still report significant delays, on the order of months, in processing NACs for their researchers who would become prospective users. This is a special problem for foreign national researchers who need to become HPC users, since they are not eligible for interim access to HPCMP systems. The resultant several months delay in obtaining access to these systems for such proposed users can waste or reduce the effectiveness of the DoD funding being provided to perform the necessary computational work on grant or contract. Additionally, an examination of usage by such individuals (academic affiliates) reflects that virtually all of the computational results obtained by these users are specifically intended for public release (i.e., the results are non-sensitive). Section 4.2 of ref (a) defines acceptable rules for usage of unclassified, non-sensitive systems. Users of non-sensitive systems must either be US citizens or foreign nationals that have been negatively screened against the Table of Denial Orders (www.ocr-inc.com Denied Parties Screening) or equivalent, and have provided their F-1 (or other type) visa number.

4. To significantly reduce these inefficiencies, the HPCMP is now establishing "open research systems," i.e. non-sensitive systems in conformity with the definition provided in para, 4.2 of ref (a), for which computational results obtained are indeed intended for public release, nominally in discipline specific research programs such as conferences, proceedings, or technical journals. These new systems designated as "open research systems" are unclassified, non-sensitive systems on which such work will be conducted.

5. DoD Directive 5200.8 outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of property or places under their command. Essential to carrying out this responsibility is a commander's need to protect the command against the action of untrustworthy persons. In accordance with above and with the above distinction between sensitive and non-sensitive systems, the requirement for all HPCMP users being required to have a "trustworthiness certification" will not be applicable for use of these open systems. However, such a requirement will continue to exist for all sensitive but unclassified systems in the HPCMP. To mitigate any risk of having foreign nationals who have not undergone a trustworthiness check on (non-sensitive and unclassified) DoD open research systems, the project leader or the government sponsor (if the project leader is non-government) will be required to certify that the work being done by these foreign nationals on the open systems is both required by a DoD contract or grant and is cleared for public release, and that the software used is not subject to export control. All other standard HPCMP security measures and access controls will remain in effect on open research systems, and all prior regulations pertaining to access and trustworthiness will apply to all other (sensitive but unclassified) HPCMP systems. As further mitigation, the HPCMP will establish a procedure for sampling

computational work being done on all of its systems to ensure that HPCMP systems are being used for their intended purposes.

3. This implementation is being made to provide more timely access to the HPCMP computing resources for a large, important segment of our user community, yet still maintaining the access restraints imperative on sensitive but unclassified systems. It will also have the effect of reducing, over time, the number of foreign nationals on DoD sensitive but unclassified HPC systems, further improving our overall security posture.

7. Accordingly, all DoD HPCMP systems at the Arctic Region Supercomputing Center will be designated "open research systems" effective 1 Oct 2004. Coincident with the date for this open system declaration, the HPCMPO security staff will have defined a process for ensuring that HPCMP systems are being used for their intended purposes.

Cray J. Henry
Director
High Performance Computing
Modernization Program